PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, H04Q 7/38

A1

(11) International Publication Number: WO 96/13920

(43) International Publication Date: 9 May 1996 (09.05.96)

(21) International Application Number: PCT/EP94/03542

(22) International Filing Date: 27 October 1994 (27.10.94)

(71) Applicant *(for all designated States except US)*: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; Old Orchard Road, Armonk, NY 10504 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: TSUDIK, Gene [US/CH]; Auf der Mauer 3, CH-8800 Thalwil (CH).

(74) Agent: BARTH, Carl, Otto; IBM Research Laboratory, Intellectual Property Dept., Säumerstrasse 4, CH-8803 Rüschlikon (CH).

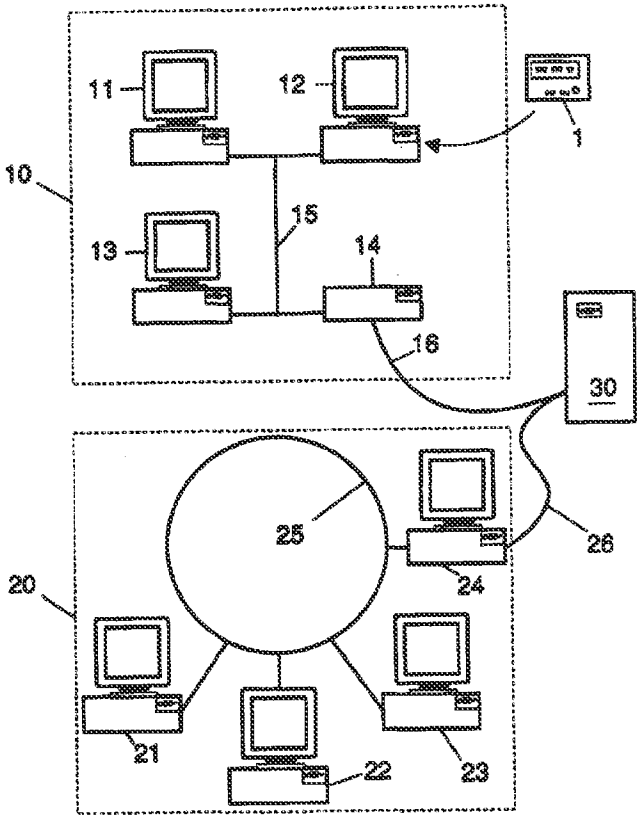
(81) Designated States: BR, CA, CN, CZ, HU, JP, KR, PL, RU, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR SECURE IDENTIFICATION OF A MOBILE USER IN A COMMUNICATION NETWORK

(57) Abstract

Communication between mobile users of and in a computer network is subject to a variety of security issues; user identification and user tracking are two particularly important ones. This invention provides a method and an apparatus for securely identifying a mobile user while avoiding trackability of his/her movements, i.e. it provides a way for a secure user identification in secrecy. The gist is to encrypt the user's identifier, and/or his/her password, and a synchronization indication, preferably a fixed time interval, under a secret one-way function and sending the encrypted message, herein called "dynamic user identifier", to the user's "home authority" where he/she is registered. The home authority comprises correspondence tables listing, pre-computed for every time interval (or another chosen synchronization), the dynamic user identifiers and the corresponding true identity of the user and can thus quickly decide whether the received encrypted message originates from a registered user. On the other hand, an intruder is neither able to detect from the encrypted messages the identity of the user nor can he/she track a user's moves.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

DESCRIPTION

Method and apparatus for secure identification of a mobile user in a communication network

Technical Field

This invention relates to communication between mobile users of and in a computer network; more specifically, it concerns a method and an apparatus for establishing a way of providing secure identification of a mobile user in a communication network.

Background of the Invention

In today's communication networks, user mobility is rapidly becoming an important and popular feature, particularly in wireless or cellular networks. While useful and desirable, this increased user mobility leads to a number of important security-related issues and concerns. One issue is the approval or acceptance of the user; another issue is the tracking a mobile user's movements and current whereabouts.

A typical situation arising in mobile environments is when an entity, i.e. a user or a device, registered in a particular home domain, appears in a different, i.e. foreign domain. Presumably, this user's goal is to obtain certain services while in the foreign domain. Since this user is not known in the foreign domain, he/she must be authenticated and his/her "solvency" or good standing must be confirmed to the authority of the foreign domain. Within the following specification, this process is denominated "authentication", as usual in the art. Of course, the only entity able to comment on the user's identity and current standing is the authority in

his/her home domain. There are several known solutions to this problem in the recent literature, some of them are addressed below. However, authentication is not the issue that the present invention addresses.

Of concern here is another security-related issue arising as a result of user mobility. It is the confidentiality of the user's identity and his/her movements. Ideally, only the user's home domain authority should be informed as to the mobile user's itinerary and current whereabouts. In the following, this process of establishing the identity of a mobile user, i.e. of determining WHO the user is trying to obtain a service from a particular domain actually, is denominated "identification".

Ideally, no entity other than the user himself/herself and a responsible authority in the user's home domain, i.e. the subnetwork or partition of the network within which the user typically works, should know the real identity and/or the current location of the mobile user. Current environments supporting user mobility either do not address the problem at all or base their solutions on hardware capabilities of the user's personal device.

Generally, one may say that the known solutions for this problem offered by current state-of-the-art mobile/cellular architectures are either inadequate or too specific to assure a secure identification in secrecy, as detailed below.

One of the presently available solutions is reported by M. Rahnema in (1). In this so-called GSM system, the mobile user is routinely assigned a temporary identity (TMSI, in GSM parlance) when he/she appears in a foreign domain. However, a TMSI is only assigned after the initial authentication of the mobile user in the foreign domain; in the process carried out by the latter, the user's real identity (IMSI, in GSM parlance) is communicated in the clear and can thus be recognized and misused by an intruder.

Another solution is described in a specification (2) on a "Cellular Digital Packet Data" (CDPD) system. The approach taken by the CDPD system is more secure than in the above GSM solution. In the CDPD system, before a mobile user communicates his/her identity, he/she engages in a Diffie-Hellman key exchange protocol with the local, i.e. foreign, domain authority. This protocol is described by W. Diffie and M Hellman in (3). As a result, both parties come to share a secret key. Enciphered under this key, the mobile user subsequently transmits his/her identity to the foreign domain authority.

While more secure than GSM, this approach has two major drawbacks. First, it allows the local, i.e. foreign, domain authority to discover the real identity of the mobile user. In the context of CDPD, this is not a problem in and of itself. However, ideally, the identity of the mobile user should not be revealed to the local domain authority. It is sufficient for establishing his/her identity and current standing if it is corroborated or endorsed by the home domain authority. The second problem is due to the nature of the Diffie-Hellman key exchange protocol. Its purpose is to establish a secret key on-the-fly. This allows an intruder to masquerade as the local domain authority and thus to engage in the key exchange protocol with the mobile user and obtain a shared key. When the mobile user then transmits its real identity enciphered with this same key, an intruder will simply decipher the transmission.

Other approaches are given by R. Molva et al in (4) and by M. Beller et al in (5). One side aspect, relating to key distribution, is described in Applicant's PCT Application PCT/EP93/01989 (6), another side aspect, relating to password or key change, is addressed in Applicant's PCT Application PCT/EP93/02540 (7).

In summary, there are essentially three issues underlying the problem of mobile user identity and movement confidentiality.

The central issue in maintaining a secret identity is to prevent anyone from discovering a correspondence between a mobile user and a user registered in a particular home domain, in other words, the central issue is to keep the user's identity confidential. The easiest, rather intuitive solution is to assign a travelling alias to every mobile user or device when away from the home domain. As addressed below, this alias can be fixed or ever-changing. Consequently, a main object of the invention is to devise a method and a system that is adapted to and permits the use of such aliases.

The second important issue is to keep foreign domains "in the dark". If it is not imperative for a foreign domain to know the real user's identity, an alias should suffice. In most cases such an alias must still be corroborated by the home domain authority. Consequently, another object of the invention is to design a method and a system which enables the information flow through the network without revealing the identity of the user to the foreign domain. (Whether or not aliases are used, there may be reasons why the foreign domain authority still demands to know the real identity of the user. In this case, the home domain authority may communicate the user's identity in secret, assuming, of course, that the two authorities have a pre-established means for secure communication. However, even in this case, the foreign domain originally does not know the user's identity.)

The third issue of particular concern is to prevent identity tracking or correlation. Even if a mobile user adopts a travelling alias, his/her movements can still be tracked by a hostile intruder. This is especially possible if the alias is fairly static, e.g. fixed for a given trip of a user or permanently allocated to said user. An alias of this latter type is similar to a long-term password; once cracked, the identity and the movements of the user can be compromised on a long-term basis. Consequently, a further object of the invention is to prevent the tracking by devising a system geared and adapted to use frequently changing aliases without inhibiting the information flow.

References

(1) Rahnema: "Overview of the GSM System and Protocol Architecture", IEEE Communications Magazine, April 1993, Vol. 31, No. 4, pp. 92-101.

(2) "Cellular Digital Packet Data (CDPD) System Specification", Release 1.0, 19 July 1993, CDPD Industry Input Coordinator, Costa Mesa, California, USA.

(3) W. Diffie and M Hellman: "New Directions in Cryptography", IEEE Transactions on Information Theory", November 1976, Vol. 22, No. 6, pp. 644-654.

(4) R. Molva, D. Samfat, G. Tsudik: "Authentication of Mobile Users", IEEE Network, Special Issue on Mobile Communications, Spring 1994, pp. 25-35.

(5) M. Beller, L. Chang, Y. Yacobi: "Privacy and Authentication on a Portable Communications System", IEEE JSAC, Special Issue on Wireless Personal Communications, August 1993, Vol. 11, No. 6, pp. 821-829.

(6) Patent Application PCT/EP93/01989, entitled "Method and Apparatus for Providing Secure Key Distribution in a Communication System", by IBM Corporation and P. Janson, G. Tsudik.

(7) Patent Application PCT/EP93/02540, entitled "Method and System for Changing an Authorization Password or Key in a Distributed Communication System", by IBM Corporation and R. Hauser, P. Janson, R. Molva, G. Tsudik, E. van Herreweghen.

(8) US National Bureau of Standards: "Federal Information Processing Standards", Publication 46, 1977.

(9) R. Rivest: "The MD5 Message Digest Algorithm", Internet RFC 1321, Internet Activities Board, April 1992.

(10) R. Molva and G. Tsudik: "Authentication Method with Impersonal Token Cards", 1993 IEEE Symposium on Research in Security and Privacy, May 1993, Proceedings published by IEEE Computer Society Press, Los Alamitos, California, USA.

(11) Security Dynamics Technologies, Inc., Cambridge, Massachusetts, USA: "The ACE System Access Control Encryption", Product Information, 1992.

Summary of the Invention

The present invention presents a solution to the above described issues. In brief, to minimize or avoid traceability and identification of a mobile user, a method of assigning temporary, simple, one-time aliases to travelling users was devised, which is both efficient and not specific to a particular hardware. The invention allows, on one hand, for unambiguous and practically instantaneous identification of the travelling user by his home authority; on the other hand, an unauthorized party is unable to identify the mobile user or track his/her movements.

Though the invention addresses and provides a comprehensive solution for all three aspects discussed above, there are still some limitations that are difficult to circumvent. One such limitation, for example, is the need of the foreign domain authority to know the identity of the home domain of the travelling user. This is likely to be the case for quite a number of mobile-user environments, since charges incurred "abroad" must be eventually propagated to the home domain. Furthermore, as mentioned before, only the home domain can comment on the user's current standing. (To solve this particular problem, one could envisage a system environment where communication between domain authorities is "anonymized" by a

central clearinghouse. In this case, it would be beneficial to assign aliases to domains so that a travelling user can reference his/her home domain by an alias; it then would be up to the central clearinghouse to resolve the domain aliases.)

The method according to the invention tries to reconcile two seemingly conflicting requirements: authentication and identity confidentiality. To authenticate an entity, it must first claim a certain identity and subsequently show or prove that it knows something that only the actual bearer of that identity can possibly know. Identity confidentiality, on the other hand, demands that the same identity be kept secret. This results in a somewhat paradoxical situation which must be solved.

In brief, the essence of the new method is in computing short-term travelling aliases, hereinafter called "dynamic user identifiers". A user travelling outside of his/her home domain can assume such an alias and hide all relationship to his real identity. Moreover, this remains to be the case even if the foreign domain (or any unauthorized party) manages to discover the travelling user's password.

Notations and Brief Description of the Drawings

Notations Used

The following notation is used throughout this description:

- D_X: domain name;
- AS_X: authority of domain D_X, typically an authentication server;
- U: travelling user, domiciled in domain D_X;
- U_X: (real) name of this travelling user U;
- A_U: alias or identifier of this travelling user U
- PW_U: user U's password
- *SUid*: dynamic user identifier

δ_X: time interval of domain x

T_U: time interval indicator, i.e. present time of user U rounded to the nearest δ value.

In the drawings is depicted in

Fig. 1 – a smartcard, useable for this invention, in both of its modes;

Fig. 2 – an example for the information flow from the smartcard to the user's home authority;

Fig. 3 – a network with two domains for demonstrating the use of the invention;

Fig. 4 – an example for the organization of the home authority's process; and

Fig. 5 – an example for the process at the foreign input workstation or terminal.

Detailed Description

Initially, every mobile user is assigned a long-term travelling alias A_U in addition to his permanent identity. In principle, A_U does not have to be different from the user's real identifier U_X; the security of the scheme does not depend on A_U being secret. In an environment where each user is equipped with a smartcard or some similar device, A_U may be nothing more than the serial number or any other unique identifier of the user's device. A list of these travelling aliases A_U is maintained by the home domain authority alongside passwords and other user information.

For every domain D_X, a domain-wide time interval δ_X is selected. This time interval δ_X can be relatively coarse, for example an hour or a day.

When a user U, whose home domain is D_x, travels to a foreign domain D_y, he/she first needs to be identified (and authenticated). Subsequently, a temporary record can be created for him/her in D_y to facilitate subsequent accesses in this foreign domain. In other words, if the user plans to linger within D_y for some time, it may be advantageous to establish some temporary "home" for him instead of having to contact the user's home domain upon every access. But this is just one further possibility. The main goal of the invention is the identification of a user.

A detailed description of a protocol for authentication of a user can be found in Molva (4) which is herewith incorporated by reference. The exact format of the authentication flows is not important in the context of the present invention. Regardless of the authentication specifics, the identity of user U must be communicated to his/her home domain authority AS_x. Since user U cannot directly communicate with the home domain authority AS_x, all communication has to flow through the local authority AS_y. This is shown in Fig. 2, described further down.

The authentication protocol may be optionally preceded by a two-flow Diffie-Hellman key change as described in the above-cited CDPD System Specification (2). In this case, the entire procedure becomes resistant to passive intruders since all messages can be enciphered using the new key.

In general, the identification flow must include the dynamic user identifier *SUid*; this is true both for the (first) flow from the smartcard/user to the foreign authority AS_y and the (second) flow from AS_y to the user's home authority AS_x. The dynamic user identification may consist of *SUid* straightaway or, possibly, an encrypted version of *SUid*.

The crucial aspect of the protocol, with respect to the confidentiality of the user's identity, is the computation of the dynamic user identifier *SUid*; it is computed as:

$$SUid = F(A_U, T_U, PW_U)$$

wherein F is a strong one-way function. Examples are DES described in Publication 46 of the National Bureau of Standards, cf. (8) above under "References", or MD5, disclosed by Rivest in (7). In case of DES or some other encryption-based function, it is important to note that no additional secret key is necessary to compute the function F since the user's password PW_U is sufficient for that purpose. T_U is the current time rounded to the nearest δ value. If the user is not equipped with a smartcard-like device, he enters his/her password PW_U into the public workstation or other such terminal, i.e. the input device connected to the foreign domain authority AS_Y. For a smartcard-bound user, PW_U can be either: 1. a strong key within the smartcard (for those smartcards that lack a keypad or other means of input), or 2. a combination of the smartcard's key and the user's password (for smartcards with input capabilities).

As specified, the dynamic user identifier value *SUid* is unintelligible to the foreign domain authority AS_Y. The only information that the foreign authority AS_Y is able to obtain is that the mobile user registered in the (home) domain D_X. In the second flow, the foreign domain authority AS_Y transmits *SUid* (along other, e.g. authentication information) to the user's claimed home domain authority AS_X.

The issue is how the home domain authority AS_X determines that *SUid* corresponds to the locally registered user U. It does so by maintaining an up-to-date table which, for each native user, lists the corresponding dynamic *SUid* value. This translation or reference table is re-computed every δ_X interval. Since the home domain authority AS_X already stores the alias A_U and the password PW_U for every user, it has all the necessary information to compute up-to-date translation tables.

It should be noted that, since the dynamic user identifiers *SUid* do not depend on the users' current location, the translation tables can be pre-computed off-line and well in advance. This is particularly the case when a relatively coarse δ_X value is used, e.g. one hour or one day, as mentioned above.

Of course, establishing the "real" identity of the mobile user is only half the work; the home domain authority AS_X must then verify the authentication information supplied in the second flow. However, this is unrelated to the problem at hand; as mentioned before, Molva et al describe an example in (4).

The following section addresses an advantageous arrangement to reduce the "computational overhead". In an environment where only few users travel outside their home domain, it can be quite inefficient and even wasteful to pre-compute, maintain, and search time-based alias tables for all users. In this case, a way to reduce overhead is to generally require a user U to inform his/her home domain authority AS_X in advance of intended travelling. Thus, the home domain authority must keep track of only those users that are currently travelling. This does not necessarily imply that users need to disclose their complete itinerary in advance; they simply need to register the beginning of each trip "abroad", i.e. to a foreign domain. Upon notification, the home domain authority AS_X adds the travelling user to a special list which is utilized for time-based dynamic identifier computation. However, it is not necessary for the user to inform his/her home domain authority AS_X upon completion of each trip; the home domain authority can deduce that a certain user has returned home when this user tries to log in with his/her real, i.e. home user ID at the home domain authority.

In the following, the clock synchronization between the home domain authority and the foreign domain authority is addressed. The assumption about the user maintaining a coarse clock, loosely-synchronized with the

home domain authority is certainly realistic for most environments. Clearly, a user equipped with a smartcard can rely on the smartcard's clock to keep track of the user time T_U. For an "unequipped" user, a workstation's internal clock will suffice. It is also possible for the user to enter the time manually from a wall-clock or a wristwatch. Of course, the granularity of δ_X is decisive. Despite this obvious ease of maintaining the user time T_U, it is conceivable that in some cases, keeping track of T_U is not possible for some reason.

To handle this situation, the protocol can be modified in a way that either, 1. the local (i.e. foreign) domain authority AS_Y provides the time T_U, or, 2. the user's home domain authority AS_X provides it. In either case, the time must be supplied to the user (or his device) a priori, i.e., in an extra flow preceding the first flow as described above. This can be done in the open, i.e. in clear text, since the time T_X is not a secret value.

To summarize, as demonstrated above, the most important factor in travelling incognito is to have frequently changing and seemingly unrelated aliases, i.e. dynamic user identifiers. As soon as constant or long-term identifiers are used, identity-correlation and tracking becomes possible. Ideally, an alias or dynamic identifier is fully disposable, i.e., use only once. The method according to the invention is not fully up to that standard because it allows aliases to be re-used within the configurable δ_X time interval. Consequently, if a user migrates through multiple domains within a single δ_X interval, he/she is vulnerable to some limited identity tracking.

To avoid this, the invention offers two alternative approaches:

1. the aliases are made dependent on the visited domain, or
2. tight synchronization between the user and his/her domain authority is maintained.

If the name of a foreign domain is included into the computation of a dynamic user identifier *SUid*, correlation of identity becomes impossible since a user migrating from one foreign domain to the next (even within a very short time, i.e. within a single time interval δ_X) will do so under unrelated dynamic user identifiers. The main drawback of this approach is that it needs more time. Since, in this case, the home domain authority AS_X is unable to predict its user's movements, it cannot pre-compute the translation tables. Thus, when the home domain authority AS_X is presented with a dynamic user identifier *SUid* and the name of the foreign domain authority D_Y, it is unable to resolve or interpret *SUid* immediately, and thus answer directly, since there is no pre-computed, stored translation table. Instead, for every registered user U, the home domain authority AS_X has to compute the appropriate *SUid* value using the name of D_Y as one of the inputs. This puts a substantial load on the home domain authority AS_X.

The other possibility is to maintain tight synchronization between the user (or, rather, personal device of the user) and the home domain authority. This synchronization can be on the basis of time, secret sequence numbers or identically-seeded random number generators. This approach provides the highest level of security since it guarantees that an alias or dynamic user identifier is never reused. It suffers, however, from the same drawback as the domain-dependent aliases. Furthermore, it requires every user to have a reliable, tamper-proof personal device.

The described time-based aliases can be realized in device-oriented environments, e.g., smartcards, cellular telephones, or in more traditional environments where a travelling user has only a password for authentication. In the latter case, a user is unavoidably vulnerable to compromised public workstations or other impersonal end-user equipment which is used to access the network. One preferred example for the implementation of the invention is given below.

A particular advantageous application of the invention is in connection with smartcards. The simplest possible smartcard is the kind that has only a small display and, perhaps, an on/off switch. Inside its tamper-proof packaging, a smartcard maintains a clock and a secret key unique for each card. This type of smartcard was described by R. Molva et al in (10). A commercial product that could be adapted to work in this mode is the SecureID token described in (11).

Implementation

Figs. 1 through 5 show an implementation of the invention with smartcards in graphical form. The following description gives the details.

Smartcard 1, shown in Fig. 1, comprises a serial number 2 which is usually fixed to the card and unique; it also comprises a processor and a display screen 3, often a small LCD, all battery powered. As explained below, smartcard 1 has two different modes; to support the time-based dynamic user identification method, the following features are provided:

1. It is programmed to switch either automatically or on demand between two modes, an "authentication mode", wherein the card displays an authenticator (not of concern here, as explained above) and a "user ID mode", wherein the card displays the dynamic user identifier *SUid*. The automatic switching occurs every so often, e.g., every ten seconds. The automatically switched smartcard is particularly attractive since it does not require any surface or hardware modifications of presently available smartcards. Alternatively, a mode button or switch 4 can be provided that allows the user to switch between the two modes.
2. The smartcard's clock used in the authentication mode is "coarsened" when computing the user identification *SUid*. A separate clock for the user ID mode is not needed, but could still be provided.

In the user ID mode, smartcard 1 displays a 6-8 digit decimal number or other sequence of symbols, shown as XX XX XXX in Fig. 1, as the time-based dynamic user identifier. This user identifier may include a preceding mark 5 to indicate that the user identifier is shown. The user duly enters this as his "user ID" into the terminal or workstation for transmission to the foreign domain authority. As mentioned below, this input step can also be carried out automatically. It should be clear at this point that the dynamic user identifier carries the user identification only in encrypted form; no intruder will be able to conclude from it the true identity of the user. It should further be clear that, since the dynamic user identifier is modified after a given time interval, any sequence of dynamic user identifiers is apparently unrelated to each other and gives no visible indication of belonging to the same user.

In the authentication mode, smartcard 1 displays another 6-8 digit decimal number or other symbol sequence, shown as YYY YYY YY in Fig.1, as the user authenticator. The user enters this authenticator as his "password" into the terminal which in turn transmits it to the foreign domain authority. (The authentication process itself, as mentioned above, is no part of this invention and will thus not be described in further detail.)

Such a smartcard could be implemented by modifying a commercially available smartcard like the SecurID card referred to in (11) which apparently already includes a clock and a processor. For someone skilled in the art, the writing of the appropriate software - if necessary - and the adaptation of the card should not pose a problem. There is not even a physical modification of the card necessary if the automatic switching from user ID mode to authentication mode is selected.

Fig. 2 shows the transmission of the dynamic user identifier and the authenticator from smartcard 1 via the foreign domain authority 6 to the user's home domain authority 8.

One preferable way is that the user inputs both values from smartcard 1, as displayed. Another way is to read the card in a terminal connected to the foreign authority 6. The usual automatic teller machines as used extensively in the banking business could be modified to do that. (Of course, for authentication, the user may also have to enter a password, PIN number, or whatever means is used by the system for the authorization process. Again, as mentioned above, the authorization process is no part of this invention; any of the conventional methods can be used.)

The foreign domain authority 6 "knows" which home domain authority it has to address. This is preferably done by including an appropriate section into the dynamic user identifier. Alternatively, a separate input can be requested from the user by foreign domain authority 6 to identify the user's home authority.

The foreign domain authority 6 transfers the data via connection 7, indicated schematically in Fig. 2 as a cable, to the user's home domain authority. Of course, this can be anything from a two-wire connection to a radio or infrared communication network. An intruder deriving data from the foreign domain authority 6 or the connection 7 will not be able to detect the user's true identity or his/her previous place of access to the system.

Since the dynamic user identifier *SUid* is already encrypted, a further encryption for a more secure transmission is not necessary, but can of course still be provided.

Fig. 3 shows a network consisting of two domains 10 and 20, each having a number of terminals or workstations for user access. The first domain 10 has a bus 15, connecting its user terminals 11 to 13 and a server 14. A link, here shown as a line or cable, connects server 14 to a gateway 30. Some or all of terminals or workstations have built-in computing power. Also, the domain authority may be distributed and not located in a particular machine or server.

The second domain 20 also has a number of terminals or workstations 21 to 24, here connected to a token ring 25. At least workstation 24 has built-in computing power and is employed as a server for this second domain. Connection 26, shown as a line, can as well be a wireless infrared or radio connection to gateway 30.

A travelling user U who wants to access the system via terminal or workstation 12, and who is "at home" in domain 20, enters his/her data, i.e. identifier, password, etc., into a keyboard or other input device at terminal 12 and/or puts his/her smartcard into a reader at the workstation. Since workstation 12 is - from the user's viewpoint - part of a foreign domain, he/she will be asked to enter his/her home domain name or it will be read from the smartcard. Either workstation 12 or, alternatively, the user's smartcard compute the dynamic user identifier *SUid*, as described above. Foreign domain authority 14 receiving this dynamic user identifier is unable to interpret it. However, it must know the user's home domain, domain 20 in the present case, in order to route or transmit the encrypted data to the correct (home) domain via gateway 30.

Gateway 30 - or any other gateway or relais station in the route - also is just able to interpret the user's correct home domain, but cannot read or interpret the dynamic user identifier *SUid*. In the present case, gateway 30 transmits the received encrypted user identifier to the user's home domain authority 24.

Domain authority 24, receiving the dynamic user identifier of its domiciled travelling user U has pre-computed up-to-date tables which list for the dynamic user identifiers for all all ist users, valid in the present time interval δ_X. Thus, by a fast and easy table look-up, domain authority can check whether the received dynamic user identifier is valid and to which user it belongs. This is described in some more detail in connection with Fig. 4. Domain authority 24 may then return an appropriate message to terminal 12

(from where the user desired service) and/or go through the authentication process.

As depicted in Fig. 4, when receiving a dynamic user identifier *SUid*, home domain authority 24 selects the appropriate alias table 42, say TB_2, from a series 41 of pre-computed tables TB_1 through TB_n according to the current time interval δ_X. It then searches the selected table using the supplied *SUid* value and identifies the serial number (or some other ID) of the smartcard or user workstation that computed *SUid*. The card serial number uniquely identifies the user. Once this identification is done, an appropriate message can be generated at domain authority 24.

Fig. 5 finally shows an example how the user's input can be processed in the input terminal 12 in the foreign domain. User U inputs his user ID or identifier A_U, his password PW_U, and, optionally, the current time T_U, rounded to the nearest time interval δ_U into workstation or terminal 12 in the foreign domain. Processing means 51, including an encryptor 52, encrypts the user's inputs, i.e. i_1 through i_3, which correspond to PW_U, A_U, and T_U, as shown in the figure. Here, the concatenation of i_1 and i_2 is encrypted under DES, referred to above in (8), under the key i_3, determining *SUid*, which is sent to the user's home domain. There, authentication server 24 evaluates the received dynamic user identifier *SUid*.

The following is a stepwise description of the full process.

STEP 0

First, and preferably permanently, each (home domain) authentication authority AS_X, typically authentication server 24, computes the tables necessary for the process. This is done every so often, e.g., once a day. Thereby, a sequence of tables, e.g. TB_1, TB_2 TB_n is computed, where n is the number of δ_X intervals in a day or other "long" time unit. For example, if δ_X is set to one hour, authentication server 24 computes 24 tables every day.

Each table TB_i, contains as many rows as there are users in the local domain. Each row consists of two columns:

- user name U, and
- the result of applying one-way function $F(A_U, T_U, PW_U)$, where PW_U is the password or PIN of user U and $T_i = T_0 \, i\delta_X$.

T_0 is the absolute time at the beginning of the computation start, i.e., if computation is done every day, then T_0 is set to midnight.

This ends the first part of the process, i.e. the table computation. The following, second part concerns the identity resolution. To enable an easy understanding, it shall be described in several steps.

STEP 1

A user U travels to a foreign domain. At a terminal or workstation in this foreign domain, say terminal 12 of domain 10 in Fig. 3, he/she enters his/her user ID U_X or alias A_U, the δ_X value, and his/her password (or PIN) PW_U into the workstation. From the input values, the workstation (software and/or hardware) computes the dynamic user identifier

$$SUid = F(A_U, T_U, PW_U),$$

where T_U is the local time on the workstation, rounded off to the nearest δ_X, i.e. seconds, minutes or hours, depending on what units δ_X is measured in. Note that it is not required for the workstation to have a clock; in that case, the user also enters the time T_U, e.g. by consulting his watch.

In addition, the user enters some authentication information into the workstation. It is not relevant to the present invention what this authentication information is.

STEP 2

The workstation sends the *SUid* value along with the authentication information to the user's home domain authority AS_X, e.g. to terminal (or workstation) 24 in domain 20. This may be done indirectly: workstation 12 can first forward the data to its own local authority AS_Y, e.g. workstation 14 of domain 10 which, in turn, then sends the data on to AS_X, here terminal or workstation 24.

STEP 3

When the data reaches AS_X, i.e. workstation 24, it first obtains its local time T_X. Then, it computes

$j = (T_X - T_0) / \delta_X$, using integer division, and

$k = (T_X - T_0) \% \delta_X$, wherein % is the modulus operator.

STEP 4

Next, AS_X, i.e. workstation 24, searches the table TB_j (pre-computed in Step 0), using *SUid* as the search value.

STEP 4a

If the search is successful, the table entry points to user U.

STEP 4b

If the search is unsuccessful, domain authority AS_X, i.e. workstation 24, may (depending on the value of k) search either TB_{j-1} or TB_{j+1}.

STEP 5

Once user U is identified, domain authority AS_X, i.e. workstation 24, verifies the authentication information that arrived along with a *SUid*, as known in the art. Again, details of this process are not relevant to the present invention.

STEP 6

When domain authority AS_x, i.e. workstation 24, is satisfied that *SUid* corresponds to a valid user U and the accompanying authentication information is correct, it responds to the remote domain authority AS_y, here server 14 in domain 10, and communicates that *SUid* is a legitimate user who is authorized to obtain service.

Obviously, the above-described process does not use a smartcard. If an "intelligent" card like smartcard 1 is to be used, the only change would be in Step 1. Instead of entering the info into the workstation, the user would simply read out the value displayed on the smartcard in its user ID mode and enter it into workstation 12. Alternatively, this value can be machine-read by workstation 12. This value is the *SUid* already computed by smartcard 1 in the same way as the workstation does it in Step 1 above.

To summarize, at the end of Step 6, domain authority AS_y, here workstation 12, can be assured that user U is a legitimate user while, at the same time, the domain authority does not and cannot discover the user's identity. In fact, domain authority AS_y only knows *SUid* which is nothing but a short-term alias. The correspondence between *SUid* and U_x is known only to the user U and his/her home domain authority AS_x.

There are obviously many variations of this invention imaginable, ranging from wireless, e.g. radio or infrared, transmission to multiplexing when serving several users simultaneously. In a wireless domain, a single server could be used as transceiver and domain authority simultaneously. Synchronization can e.g. be achieved by radio-controlled clocks or other synchronization devices. Smartcards could be carrying any meaningful computing power in order to make the terminals as robust as possible. All these variations could still be using the essential principles of this invention as defined in the appended claims.

CLAIMS

1. A method for secure identification of a mobile user U in a communication system with a plurality of distributed users grouped to domains or subsets D_X, D_Y within the system, each said user having an identifier A_U and a password or other secret authenticator PW_U, said identifier and said password being stored in said user's home domain D_U, said method including a synchronization indication, preferably applying a time interval indication T_U, synchronizing said user's U input in a foreign domain D_Y with his/her home domain D_U,

comprising the steps of:

- encrypting under a secret function, particularly a one-way function, at least one of the group consisting of said identifier A_U, said time interval or other synchronization indication T_U, and said user's password PW_U or other secret authenticator, and building an encrypted message,
- indicating to said foreign domain D_Y, from which said user U intends to communicate, said user's home domain D_U,
- - transmitting said encrypted message to said user's home domain D_U,
- evaluating in said user's home domain D_U said encrypted message and determining the true identity of said user.

2. The identification method of claim 1, with distributed workstations and/or terminals (11-14, 21-24) grouped to domains or subsets D_X, D_Y (10, 20) within the system, wherein
the encryption step is carried out in the foreign domain D_Y and the encrypted message transmitted to said user's home domain D_U for the evaluation.

3. The identification method of claim 1, using "intelligent" portable input means, preferably smartcards (1), with built-in computing power, wherein
the encryption is carried out in said portable input means and the encrypted message transmitted to said user's home domain D_U for the evaluation.

4. The identification method of claim 3, wherein
at least part of the entry into the foreign domain D_Y is done from the portable input means, preferably by machine-reading the latter.

5. The identification method of any of the claims 1 through 3, wherein
- if the determining step is successful, an approval message from the home domain D_U is transmitted, in particular to the foreign domain D_Y,
- if the determining step is unsuccessful, an appropriate disapproval is indicated.

6. The identification method of claim 1, wherein
- the secret function is a one-way function
$SUid = F(A_U, T_U, PW_U)$
encrypting the identifier A_U, the time interval indication T_U or other synchronization indication, and the user's password PW_U or other secret authenticator, and/or
- the identifier A_U is an alias or secondary identifier of user U.

7. The identification method of any preceding claim, wherein
in the home domain D_U, prior to a respective time interval δ_U or other synchronization interval indication, one or more potential encrypted messages for a future time interval are pre-computed and stored in a reference/translation table (42).

8. The identification method of claim 7, wherein
the reference/translation table (42) in the home domain D_U is established selectively, in particular only for selected mobile users known to be moving.

9. The identification method of claim 1, wherein
for each domain D_X, a domain-wide time interval δ_X is selected, said selected time interval being one or more hours or a day.

10. The identification method of claim 1, wherein
the synchronization means includes identically seeded random-number generators and/or secret sequence numbers.

11. A portable input means, in particular a smartcard (1), adapted for use in a communication system according to any of the claims 1 - 10, having a secret key unique for each input means and a clock, further comprising means for switching said input means between an identification mode and a user ID mode in which it displays the encrypted message.

12. The input means of claim 11, wherein
switching said input means is done by a manual mode switch (4) for manually switching said input means between its modes and/or an automatic mode switch for automatically switching said input means time-dependant between its modes.

13. A system for secure identification of a mobile user in a communication network including a plurality of distributed workstations or terminals (11-14, 21-24) grouped to domains or subsets D_X, D_Y (10, 20) within said network, said user having an identifier A_U and a secret authenticator PW_U,

- means for encrypting (Fig. 5) under a secret function, particularly a one-way function, at least one of the group consisting of said identifier A_U, a synchronization indicator T_U, and said user's

authenticator PW_U, for building a first message, and indicating said user's home domain D_U,

- means for transmitting (16, 26, 30) said first message to said user's home domain D_U,
- means for receiving (Fig. 4) in said user's home domain D_U (20) said first message, and determining the true identity of said user U.

14. The identification system of claim 13, wherein

message control and handling within the foreign domain D_y (10) and/or within the home domain D_U (20) is done within and by a domain authority or an identification server AS_y (14) or AS_U (24), respectively.

15. The identification system of claim 13, including

in a domain authority AS_U (24), means (41) for storing a plurality of the translation tables (42).

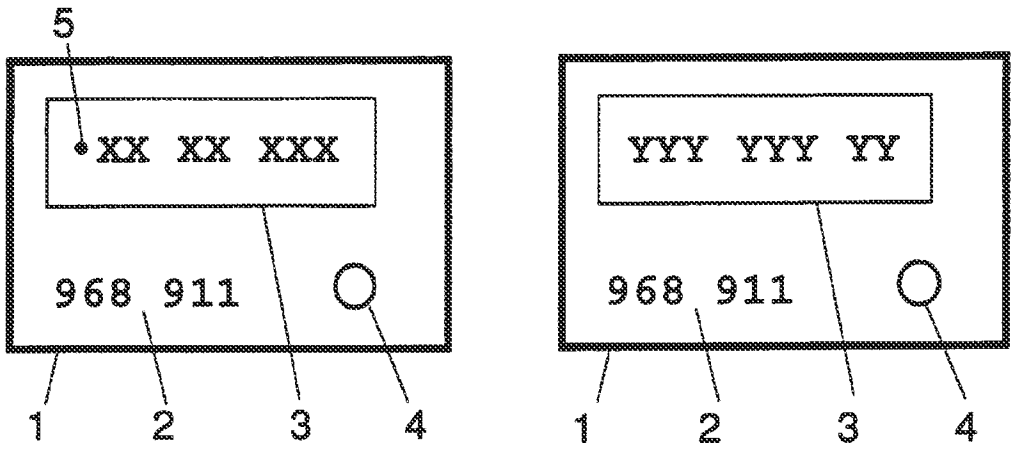

5
XX XX XXX
968 911
1
2
3
4
YYY YYY YY
968 911
1
2
3
4

Fig.1

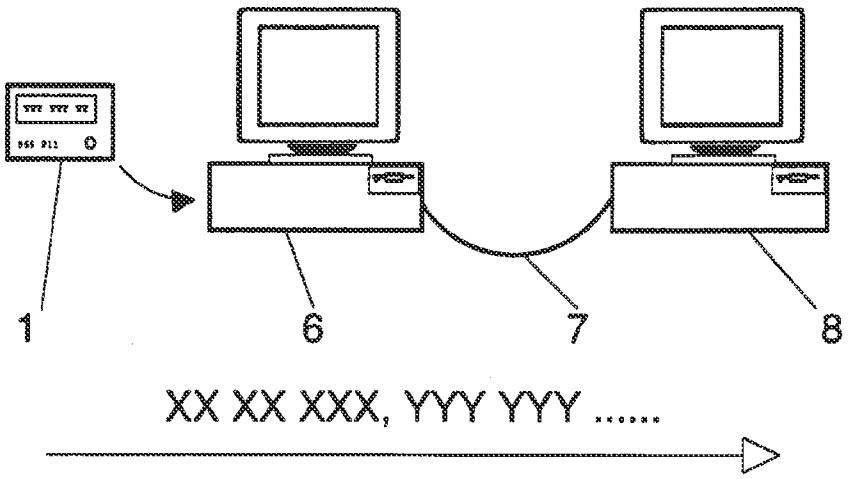

1
6
7
8
XX XX XXX, YYY YYY .....

Fig.2

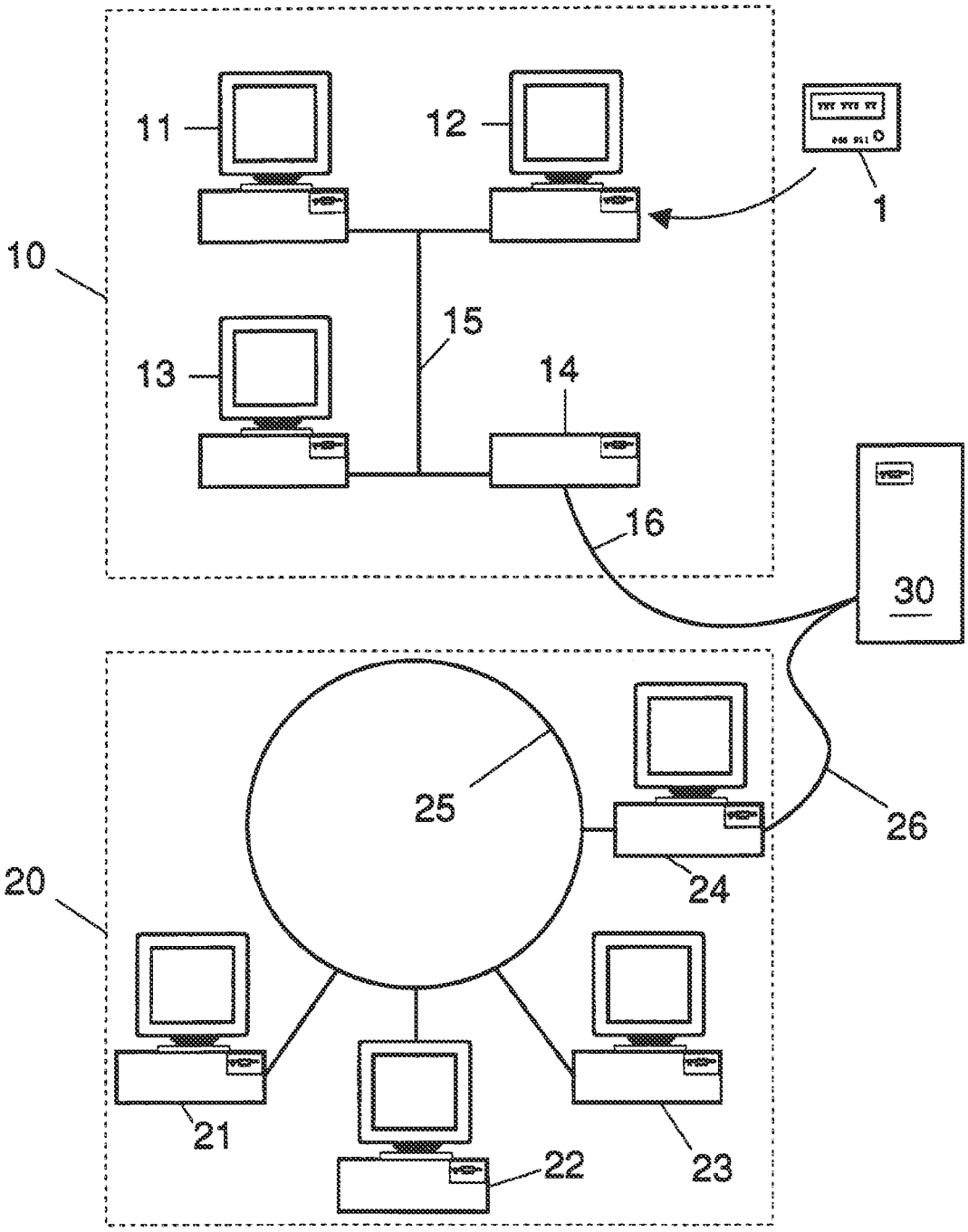


Fig.3

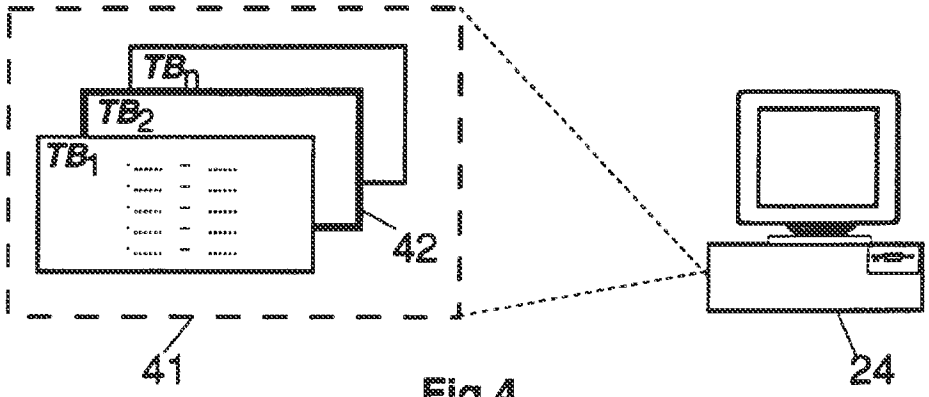


Fig.4

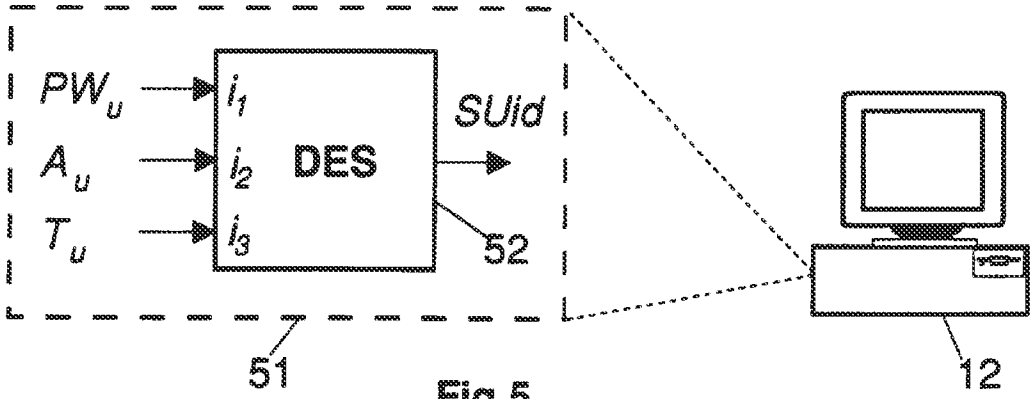


Fig.5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 94/03542

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS, March 1994 - April 1994 NEW YORK US, pages 26-34, R.MOLVA ET AL. 'AUTHENTICATION OF MOBILE USERS' cited in the application see page 26, left column, line 1 - line 20 see page 30, left column, line 14 - line 18 see page 32, right column, line 32 - page 33, left column, line 31 -/--	1,13

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 August 1995	04.10.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Lydon, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PC./EP 94/03542

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP-A-0 532 227 (AMERICAN TELEPHONE AND TELEGRAPH COMPANY) 17 March 1993 see page 3, column 3, line 30 - line 55 see page 3, column 4, line 53 - page 4, column 5, line 39 see page 4, column 6, line 10 - line 17 see page 5, column 7, line 6 - column 8, line 8 see page 5, column 8, line 38 - page 6, column 9, line 31 see page 8, column 13, line 50 - column 14, line 4 see figures 1,2,11	1,13
A	PROCEEDINGS OF GLOBECOM'93 - IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE HOUSTON(US), 29 November 1993 - 2 December 1993 NEW YORK (US), pages 550-554, H.-Y.LIN & L.HARN 'AUTHENTICATION IN WIRELESS COMMUNICATIONS' see page 551, left column, line 15 - line 45 see page 551, right column, line 3 - page 552, left column, line 23 see page 552, left column, line 41 - page 553, left column, line 12 see figures 1-3	1,13
X	COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY., vol. 6, no. 1, February 1987 AMSTERDAM NL, pages 10-11, J.H.HIGHLAND 'TECHNOLOGY WATCH - PERSONAL AUTHENTICATION DEVICES' see page 11, left column, line 13 - line 26 see figure 3	11,12
A	PROCEEDINGS OF 1993 IEEE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY OAKLAND (US) 24-26 MAY 1993 NEW YORK (US), pages 56-65, R.MOLVA & G.TSUDIK 'AUTHENTICATION METHOD WITH IMPERSONAL TOKEN CARDS' cited in the application see page 59, paragraph 5.1 see figure 1	12

3

INTERNATIONAL SEARCH REPORT

national application No.
PCT/EP 94/03542

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. Claims 1-10, 13-15: A method and system for secure identification of a mobile user in a communication network.
2. Claims 11-12: A portable input means with means for switching between an authentication mode and a user ID mode.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searches without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☒ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int onal Application No
PCT/EP 94/03542

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-532227	17-03-93	US-A-	5204902	20-04-93
		JP-A-	6188828	08-07-94